Technische Aspekte der IT-Sicherheit

Mirko Wollenberg (DFN-CERT Services GmbH)

An der fiktiven Hochschule Pellworm geht nichts mehr: Das Immatrikulationsamt kann nicht auf die Studierendendaten zugreifen. Das Institut für Hochenergiephysik kann die neusten Messdaten vom Large Hadron Collider am CERN nicht herunterladen. Die Biologen verpassen die Deadline für die elektronische Einreichung des für die Bewerbung bei der Exzellenzinitiative wichtigen Beitrags für das Nature Magazine. Was ist passiert? Schnell wird klar: Ein Angriff auf die Informationssysteme der Hochschule ist schuld - trotz umfangreicher präventiver Sicherheitsmaßnahmen. Potentielle Angreifer gibt es viele: Ist es eine exmatrikulierte Studentin, die sich an der Hochschule rächen will? Ein konkurrierendes ausländisches Forschungsinstitut, das ein bahnbrechendes Forschungsergebnis zuerst veröffentlichen möchte? Oder eine kriminelle Vereinigung, die die Hochschule erpressen möchte? Nachdem die Krisenprozesse der Hochschule gestartet wurden, lichtet sich der Nebel schließlich: Der Angriffsvektor kann mit Hilfe einer Logfile-Analyse identifiziert und die Infektion der betroffenen Systeme entfernt werden. Nach und nach werden die kritischen Systeme wieder erfolgreich in Betrieb genommen. Trotzdem entsteht ein signifikanter Schaden: Nicht nur finanziell, sondern auch die Reputation der Hochschule leidet. Daher müssen auch Managementsysteme für Informationssicherheit und Datenschutz kontinuierlich weiterentwickelt und verbessert werden. Hierzu braucht man externe Unterstützung und Hilfsmittel. Viele hiervon bietet der DFN-Verein seinen Teilnehmern im Rahmen der DFN-Dienste an und mehr ist in Vorbereitung.

Dieser Vortrag gibt einen Überblick über diese DFN-Dienste und die zukünftige Entwicklung.